Claims

1   1.   A method of managing the secure mutual configuration of a plurality of

2   servers interconnected by a communications network, said method comprising the

3   steps of:

4   a) routinely exchanging status messages between said plurality of servers

5   wherein said status messages identify changes in the mutual configuration of said

6   plurality of servers, wherein each said status message includes encrypted

7   validation data and wherein said plurality of servers stores respective

8   configuration data including respective sets of data identifying the servers known

9   to the respective servers as constituting said plurality of servers;

10   b) validating status messages as respectively received by said plurality of

11   servers against the respective configuration data stored by said plurality of servers

12   wherein status messages are determined valid when originating from a first server

13   as determined known relative to the respective configuration data of a second

14   server; and

15   c) selectively modifying the respective configuration data of said second

16   server.

1   2.   The method of Claim 1 wherein said step of selectively modifying includes

2   the steps of:

3   a) retrieving the respective configuration data of said first server; and

4   b) incorporating the respective configuration data of said first server as the

5   respective configuration data of said second server.

- 47 -

1　3.　　The method of Claim 2 wherein the respective configuration data of said
2　first server includes encrypted validation data and wherein said step of retrieving
3　includes the step of validating the respective configuration data of said first server
4　as originating from a known server of said plurality of servers as determined
5　relative to the respective configuration data of a second server.

1　4.　　The method of Claim 3 wherein said known server is said first server.

1　5.　　The method of Claim 4 wherein the encrypted validation data included in
2　the respective configuration data is a digital signature of the respective
3　configuration data.

1　6.　　The method of Claim 5 wherein the encrypted validation data included in
2　the status messages includes an encrypted identifier of the respective servers
3　originating the status messages.

1　7.　　The method of Claim 6 the method of Claim 6 wherein the respective
2　configuration data includes respective sets of the public keys corresponding to the
3　servers known to the respective servers as constituting said plurality of servers.

1　8.　　The method of Claim 7 wherein the status messages include respective
2　configuration data version identifiers and wherein said step of retrieving is
3　responsive to configuration data version identifiers that are more current the
4　configuration data version identifier of the respective configuration data held by
5　a respective server of said plurality of servers.

1 9.   The method of Claim 8 wherein a predetermined server of said plurality of

2 servers includes an administrative interface through which the   respective

3 configuration data may be modified, said method further comprising the step of

4 revising the respective configuration data version identifier of administratively

5 modified configuration data.

1 10.   A   method   of   securely   distributing   configuration   data   over   a

2 communications network to a plurality of computer systems, each computer

3 system operating to evaluate configuration data, as stored in respective

4 configuration data stores, in response to service requests to determine respective

5 responses, said method comprising:

6   a) receiving, by a computer system, a version message from said

7 communications network;

8   b) verifying said version message using verification   encryption data

9 securely held by said computer system;

10   c) determining, based on said version message, to retrieve updated

11 configuration data from a configuration data source server identified relative to

12 said a version number message; and

13   d) installing updated configuration data to the configuration data store of

14 said computer system as retrieved from said configuration data source server,

15 wherein said updated configuration data is retrieved as an encrypted data block

16 and wherein said step of installing includes locating predetermined configuration

17 data within said encrypted data block and decrypting said predetermined

18 configuration data.

1   11.   The method of Claim 10 wherein said locating step determines the location

2   of said predetermined configuration data using location encryption data securely

3   held by said computer system.

1   12.   The method of Claim 11 wherein said verification encryption data and said

2   location encryption data are related to a private encryption key securely held by

3   said computer system.

1   13.   The method of Claim 12 wherein said verification encryption data and said

2   location encryption data are related to respective private encryption keys securely

3   held by said computer system.

1   14.   The method of Claim 10 wherein said plurality of computer systems use

2   a common version of said configuration data, wherein said step of installing

3   finally installs said updated configuration data for use by said computer system

4   and wherein said method further comprises the steps of:

5   a) staging said updated configuration data pending completion of the

6   installation of said updated configuration data; and

7   b) waiting for said plurality of computer systems to signal use of a common

8   version of said configuration data whereupon said step of installing completes the

9   installation of said updated configuration data.

1   15.   The method of Claim 14 wherein said computer system receives version

2   message from each of the other ones of said plurality of computer systems,

3   wherein said step of determining determines the latest version of configuration

4   data in use or staged for use by each of the other ones of said plurality of

5   computer systems, and wherein said step of waiting waits for each of the other

6   ones of said plurality of computer systems to signal use of a common latest

7   version of said configuration data.

1   16.   The method of Claim 15 wherein said plurality of computer systems to

2   signal use of a common latest version of said configuration data through

3   respective version messages.

1   17.   A method of securely distributing configuration information through a

2   communications network among a cluster of computer systems providing a

3   network service, wherein configuration information modifications are distributed

4   from a computer system participating in the cluster and mutually coordinated in

5   installation in the participating cluster computer systems to enable a consistent

6   configuration information versioned operation of said cluster of computer systems,

7   said method comprising:

8   a) receiving a modified configuration data set having a predetermined

9   configuration version;

10   b) preparing an encrypted configuration data set by encrypting said

11   modified configuration data set using predetermined encryption keys

12   corresponding to encryption key data included in said modified configuration data

13   set;

14   c) sending a configuration version message, referencing said

15   predetermined configuration version, over the communications network

16   connecting the cluster of computer systems;

17   d) servicing requests to retrieve a copy of said encrypted configuration data

18   set; and

19   e) coordinating, among the cluster of computer systems, installation of said

20   modified configuration data set as the operative configuration data set of the

21   computer systems of the cluster.

1   18.   The method of Claim 17 wherein the computer systems of said cluster

2   respectively execute a common network service application, wherein execution of

3   said common network service application is dependent on a respective installed

4   configuration data set, and wherein said step of coordinating provides for the

5   mutually corresponding installation of said modified configuration data set by said

6   computer systems whereby execution of said common network service application

7   is consistent across the cluster of computer systems.

1   19.   The method of Claim 18 wherein said modified configuration data set

2   includes individual configuration data sets identified with respective computer

3   systems of the cluster, wherein said modified configuration data set includes a

4   plurality of private encryption keys and wherein said step of preparing provides

5   for the encryption of said modified configuration data using said plurality of

6   private encryption keys.

1   20.   The method of Claim 19 wherein said individual data sets are encrypted

2   relative to respective ones of said plurality of private encryption keys and wherein

3   a predetermined computer system of said cluster must have a respective one of

4   said plurality of private encryption keys to decrypt a corresponding one of said

5   individual data sets from said encrypted configuration data set.

1   21.   A method of securely distributing configuration data sets among server

2   computer systems of a server cluster, wherein an operative configuration data set

3   is used by an individual server computer system to define the parameters for

4   executing a network service by that server computer system, said method

5   comprising the steps of:

6   a) identifying, by a first server computer system of said server cluster, a

7   revised configuration data set held by a second server computer system of said

8   server cluster;

9   b) retrieving, by said first server computer system, said revised

10   configuration data set from said second server computer system;

11   c) decrypting said revised configuration data set for installation as a current

12   configuration data set for said first server computer system, said revised

13   configuration data set having been uniquely encrypted for decryption by said first

14   server computer system;

15   d) verifying, by said first server computer system, that each server computer

16   system of said server cluster has said current configuration data set; and

17   e) installing said current configuration data set on said first server computer

18   system as the operative configuration data for said first server computer system.

1 22. The method of Claim 21 wherein said revised configuration data set

2 includes a plurality of respectively encrypted current configuration data sets and

3 wherein said step of decrypting includes the steps of:

4   a) locating said current configuration data set, as encrypted uniquely for

5 said first server computer system, from among said plurality of respectively

6 encrypted configuration data sets; and

7   b) discretely decrypting said current configuration data set from said

8 revised configuration data set.

1 23. The method of Claim 22 wherein said first server computer system has a

2 unique private decryption key and wherein said step of locating depends on the

3 identification, by said first server computer system, of a representation of said

4 unique private decryption key in said revised configuration data set, whereby

5 location and decryption of said plurality of respectively encrypted current

6 configuration data sets is locked to the respective server computer systems of said

7 server cluster.

1 24. The method of Claim 23 wherein said revised configuration data set

2 includes representations of the unique private decryption keys of the respective

3 server computer systems of said server cluster and wherein said step of locating

4 includes:

5   a) matching a predetermined representation of said unique private

6 decryption key of said first server computer system with a corresponding one of

7 said representations of said revised configuration data set; and

8   b) determining, based on the matched representation of said unique

9 private decryption key of said first server computer system, the location of said

10 current configuration data set, as encrypted, from among said plurality of

11 respectively encrypted configuration data sets.

1 25.   The method of Claim 24 wherein said representations of the unique private

2 decryption keys are secure digests of the unique private decryption keys of the

3 respective server computer systems of said server cluster.

1 26.   The method of Claim 21 wherein said operative configuration data set

2 includes a first version identifier and wherein said step of identifying includes:

3   a) receiving, by said first server computer system, version messages from

4 the other server computer systems of said server cluster, wherein each version

5 message includes a second version identifier and identifies a version message

6 source server computer system; and

7   b) determining, with respect to a predetermined version message, whether

8 said second version identifier, relative to said first version identifier, corresponds

9 to said revised configuration data set.

1 27.   The method of Claim 26 wherein said step of identifying further includes

2 a step of validating said version messages with respect to said first server

3 computer system.

1 28.   The method of Claim 27 wherein said first server computer system has a

2 unique private decryption key and wherein said step of validating depends on the

3   identification, by said first server computer system, of a representation of said

4   unique private decryption key in said version messages such that version

5   messages lacking said representation are discarded by said first computer server

6   computer system.

1   29.   The method of Claim 28 wherein said version message includes

2   representations of the unique private decryption keys of the respective server

3   computer systems of said server cluster and wherein said step of validating

4   includes matching said representation of said unique private decryption key of

5   said first server computer system with a corresponding one of said representations

6   of said revised configuration data set.

1   30.   The method of Claim 29 wherein said representations of the unique private

2   decryption keys are secure digests of the unique private decryption keys of the

3   respective server computer systems of said server cluster.

1   31.   The method of Claim 30 wherein said revised configuration data set

2   includes said representations of the unique private decryption keys and a plurality

3   of respectively encrypted current configuration data sets, wherein said step of

4   decrypting includes the steps of:

5   a) matching, by said first server computer system, of said predetermined

6   representation of said unique private decryption key of said first server computer

7   system in said revised configuration data set;

8   b) determining, based on the matched representation of said unique

9   private decryption key of said first server computer system, the location of said

10 current configuration data set, as encrypted, from among said plurality of

11 respectively encrypted configuration data sets; and

12   c) discretely decrypting said current configuration data set from said revised

13 configuration data set, whereby the location and decryption of said plurality of

14 respectively encrypted current configuration data sets is locked to the respective

15 server computer systems of said server cluster.

1   32.   A server computer system coupleable through a communications network

2   as part of a computer system cluster to support performance of a network service

3   on behalf of a client computer system, said server computer system comprising:

4   a) a processor operative to execute control programs; and

5   b) a service program operative, through execution by said processor as a

6   control program,

7   to generate responses to predetermined client requests,

8   wherein responses are generated based on an evaluation of an

9   installed configuration data set,

10   said service program being further operative to implement a secure

11 network protocol, interactive with said computer system cluster, to identify and

12 receive an updated configuration data set for installation as said installed

13 configuration data set,

14   said service program including a unique private encryption key,

15   wherein said secure network protocol provides for the transfer of an

16 encrypted configuration data block including a plurality of encrypted updated

17 configuration data sets, a respective one of said plurality of encrypted updated

18 data sets being decryptable using said unique private encryption key.

1   33.   The server computer system of Claim 32 wherein said service program is

2   operative to first locate and second decrypt said respective one of said plurality

3   of encrypted updated data sets based on said unique private encryption key.

1   34.   The server computer system of Claim 33 wherein said encrypted

2   configuration data block includes a plurality of location references, wherein said

3   service program is operative to associate said unique private encryption key with

4   a corresponding one of said plurality of location references, said service program

5   being further operative to locate said respective one of said plurality of encrypted

6   updated data sets based on said corresponding one of said plurality of location

7   references.

1   35.   The server computer system of Claim 34 wherein said corresponding one

2   of said plurality of location references is a secure digest of said unique private

3   encryption key.

1   36.   The server computer system of Claim 34 wherein said service program is

2   operative to determine whether to receive said updated configuration data set.

1   37.   The server computer system of Claim 36 wherein said installed

2   configuration data set has a first version identifier, wherein said updated

3   configuration data set has a second version identifier, said service program being

4   responsive to said first and second version identifiers to determine whether to

5   receive said updated configuration data set.

1   38.   The server computer system of Claim 37 wherein said service program is

2   operative, in response to administrative modifications that produce said updated

3   configuration data set, to generate said encrypted configuration data block with

4   said second version identifier, said service program being further operative to

5   provide a version message containing said second version identifier to said

6   computer system cluster and responsive to requests to transfer said encrypted

7   configuration data block.

1   39.   The server computer system of Claim 37 wherein said service program is

2   operative to successively broadcast said version message.

1   40.   The server computer system of Claim 39 further comprising a first network

2   connection coupleable to said client computer system and a second network

3   connection coupleable to said computer system cluster, wherein said second

4   network connection is utilized to successively transfer said version message and

5   to transfer said encrypted configuration data block.

1   41.   The server computer system of Claim 40 further comprising a third network

2   connection accessible by an administrator for applying administrative

3   modifications that produce said updated configuration data set.

1   42.   A method of securely constraining participation of select computer systems

2   in the cooperative operation of a server cluster to insure the integrity of the

gbr/aesn/3013.000.utility.wpd

7/17/2003

3   information transactions among the computer systems of said server cluster, said

4   method comprising the steps of:

5   a) receiving, by a first computer system of a server cluster, a request for the

6   transfer of first specified data, held in a first secure memory store of said first

7   computer system, to a second computer system of said server cluster;

8   b) transmitting, by said first computer system, encrypted information

9   including said first specified data to said second computer system, wherein said

10 encrypted information, as prepared by said first computer system, is further

11 encoded to include a first secure discrete reference;

12   c) verifying said first secure discrete reference against a second secure

13 discrete reference determinable from second specified data stored in a second

14 secure memory store of said second computer system;

15   d) locating, by said second computer system with respect to said first secure

16 discrete reference, a predetermined subset of said encrypted information

17 decryptable by said second computer system to recover said first specified data;

18 and

19   e) installing said first specified data in said second secure memory store of

20 said second computer system.

1   43.   The method of Claim 42 wherein said request and said encrypted

2   information are transferred over a communication network interconnecting the

3   computer systems of said server cluster.

1 44.   The method of Claim 43 wherein said first and second secure discrete

2 references are secure digests of a secure private encryption key assigned to said

3 second computer systems.

1 45.   The method of Claim 44 wherein said first and second specified data

2 respectively includes said first and second secure discrete references.

1 46.   The method of Claim 44 wherein said first and second specified data

2 includes said secure private encryption key.

1 47.   The method of Claim 44 wherein each of the computer systems of said

2 server cluster are assigned unique secure private encryption keys and wherein a

3 set of secure discrete references, including said first and second secure discrete

4 references, corresponding to the set of unique secure private encryption keys are

5 determinable from the respective specified data stored by said computer systems

6 of said server cluster.

1 48.   The method of Claim 47 wherein the set of unique secure private

2 encryption keys are stored in each of the respective specified data stored by said

3 computer systems of said server cluster.

1 49.   The method of Claim 47 wherein the respective specified data stored by

2 said computer systems of said server cluster are versioned, said method further

3 comprising the steps of:

4   a) identifying, by said second computer system, that said first specified data

5 is a later version relative to the version of said second specified data; and

6   b) requesting, by said second computer system, said first specified data

7 from said first computer system.

1 50. The method of Claim 49 further comprising the step of coordinating,

2 relative to others of said computer systems of said server cluster, the installation

3 of said first specified data by said second computer system.

1 51. The method of Claim 50 wherein said step of identifying further identifies

2 said first specified data as the latest available version of the respective specified

3 data.

1 52. The method of Claim 50 wherein said second computer system nominally

2 responds to predetermined client requests, said method further comprising the

3 step of declining, by said second computer system, said predetermined client

4 requests in the interim between said step of identifying and said step of installing.

1 53. A method of distributing configuration control data among a cluster of

2 computer systems to ensure consistent operation of the cluster in response to

3 network requests received from host computers, wherein each computer system

4 maintains a local control data set that, in active use, determines the functional

5 operation of the respective computer system, and wherein said cluster of computer

6 systems and said host computers are interconnected by a communications

7 network, said method comprising the steps of:

8   a) storing, in a first computer system of a cluster of computer systems, a

9   first local control data set having a predetermined version number;

10   b) transmitting a cluster message including said predetermined version

11   number from said first computer system to said cluster of computer systems;

12   c) transferring said first local control data set to requesting computer

13   systems of said cluster of computer systems; and

14   d) synchronizing with said requesting computer systems the installation of

15   said first local control data set for active use by said requesting computer systems.

1   54.   The method of Claim 53 further comprising the step of changing said

2   predetermined version number in connection with a predetermined modification

3   of said first local control data set, wherein said requesting computer systems are

4   responsive to the change in said predetermined version number.

1   55.   The method of Claim 54 wherein said step of synchronization includes the

2   steps of:

3   a) providing, respectively by said requesting computer systems, readiness

4   signals to said cluster to establish a readiness to install said first local control data

5   set; and

6   b) establishing, respectively by said requesting computer systems, receipt

7   of said readiness signals from all of said requesting computer systems to enable

8   respective installation of said first local control data set for active use.

1   56.   The method of Claim 55 wherein each actively participating computer

2   system of said cluster routinely performs said step of transmitting, wherein each

12   b) transmitting, mutually among said computer systems of said cluster,

13 cluster messages including respective representations of said predefined version

14 values;

15   c) supporting, with respect to a predetermined computer system of said

16 cluster, provision of a updated configuration data set for installation as said active

17 configuration data set, said updated configuration data set having an updated

18 version value, and wherein said cluster messages transmitted by said

19 predetermined computer system reflect said updated version value;

20   d) propagating said updated configuration data set from said

21 predetermined computer system among said computer systems of said cluster;

22 and

23   e) coordinating the installation of said updated configuration data set as

24 said active configuration data set in each of said computer systems of said cluster.

1   60.   The method of Claim 59 wherein said step of coordinating provides for the

2   installation of said updated configuration data set determined respectively based

3   on a convergence of the version values received in said cluster messages from the

4   computer systems of said cluster.

1   61.   The method of Claim 60 wherein said provision of said updated

2   configuration data set includes administrative provision.

1   62.   The method of Claim 61 wherein said provision of said updated

2   configuration data set includes a modification of the local active configuration

3   data set.

1   63.   The method of Claim 62 wherein said step of coordinating provides for the

2   respective installation of said updated configuration data set by the computer

3   systems of the cluster once a respective computer system receives a predetermined

4   number of said cluster messages from each of the other computer systems of said

5   cluster each including said updated version value.

1   64.   The method of Claim 63 wherein said predetermined number is two.

2   65.   A method of securely establishing consistent operation of a networked

3   cluster of computer systems to provide a network service on behalf of host

4   computer systems, said method comprising the steps of:

5   a) enabling distribution of an updated configuration data set among a

6   cluster of computer systems, wherein each said computer system is operative

7   against a respective active configuration data set, and wherein respective

8   instances of said updated configuration data set are received and held by said

9   cluster of computer systems pending installation as said respective active

10 configuration data sets;

11   b) determining, by each said computer system, when a predetermined

12 installation criteria is met with respect to each said computer system; and

13   c) installing said respective instances of said updated configuration data

14 set as said respective active configuration data sets.

1   66.   The method of Claim 66 wherein said step of enabling distribution includes

2   a step of transmitting a message to said cluster of computer systems and wherein

3   said message is encrypted so as to be readable only by those computer systems

4   of said cluster that are predetermined valid participants in said cluster.

1   67.   The method of Claim 67 wherein said message, as prepared by a first

2   computer systems of said cluster, is encrypted so as to be readable only by second

3   computer systems of said cluster that are preestablished to said first computer

4   system as valid participants of said cluster.

1   68.   The method of Claim 68 further comprising the step of preparing, by said

2   first computer system, said message utilizing encryption codes respectively

3   corresponding to said second computer systems.

1   69.   The method of Claim 69 wherein said first computer system securely stores

2   a preestablished set of public key encryption codes corresponding to said second

3   computer systems and wherein said second computer systems are only responsive

4   to said message where said message stores a secure representation of the

5   respective public key encryption code of a corresponding one of said second

6   computer systems that receives said message.

1   70.   The method of Claim 65 further comprising the steps of:

2   a) storing, by a first computer system of said cluster, a set of encryption

3   codes corresponding to second computer systems of said cluster, said set of

4   encryption codes being preestablished, representing predetermined valid

5   participants in said cluster, and securely stored by said first computer system;

6   b) preparing, by said first computer system, a message for distribution to

7 said second computer systems, said message including secure representations of

8 said encryption codes;

9   c) transmitting said message to said cluster; and

10   d) validating said message by said second computer systems upon

11 recognizing respective instances of said representations of said encryption codes.

1 71.   The method of Claim 70 further comprising the step of retrieving, by a

2 predetermined second computer system, a copy of said set of encryption codes

3 from said first computer system for use by said predetermined second computer

4 system subsequently in the role of said first computer system.

1 72.   The method of Claim 71 wherein said secure representations are secure

2 hashes of the public keys of said second computer systems.

1 73.   A method of securely constraining participation of select computer systems

2 in the operation of a server cluster, interconnected by a communications network,

3 to insure the security of configuration information distributed among the computer

4 systems of said server cluster, said method comprising the steps of:

5   a) storing, by a first computer system of a server cluster, first specified data

6 within a secure memory store, said first specified data being identified by a first

7 version identifier;

8   b) receiving, by said first computer system, a cluster message including a

9 second version identifier and verification data from a second computer system of

10 said server cluster;

11   c) verifying, by said first computer system, said cluster message by

12 evaluation of said verification data relative to said first specified data;

13   d) obtaining, from said second computer system, dependent on a

14 successful verification of said verification data, encrypted information including

15 second specified data corresponding to said second version identifier;

16   e) decrypting said second specified data from said encrypted information;

17 and

18   f) incorporating said second specified data into said secure memory store

19 of said first computer system, whereby the operation configuration of said first

20 computer system is securely made consistent with that of said second computer

21 system.

1 74.   The method of Claim 73 wherein said first and second specified data is

2 configuration information that, as incorporated in said secure memory store,

3 determines the operational performance of said first computer system of said

4 server cluster in responding to network requests issued by any of a plurality of host

5 computer systems to obtain a performance of a network service.

1 75.   The method of Claim 74 wherein said first specified data includes a

2 predetermined set of encryption codes corresponding to the validly participating

3 computer systems of said server cluster as known to said first computer system,

4 and wherein said step of validating said cluster message includes requiring the

5 valid decryption of said verification data using an encryption code of said

6 predetermined set identified with said second computer system, whereby cluster

7   messages are accepted as valid by said first computer system only from

8   preestablished validly participating computer system of said server cluster.

1   76.   The method of Claim 75 wherein changes to said predetermined set of

2   encryption codes are constrained to secure update procedures including

3   incorporation of said second specified data into said secure memory store and

4   administrative operations securely executed against a computer system of said

5   server cluster, whereby configuration data is securely maintained and distributed

6   only among the computer systems of said server cluster of administratively

7   preestablished identity.

1   77.   The method of Claim 76 wherein said verification data includes a

2   predetermined cipher text encrypted to ensure secure identification of said request

3   as originating from said second computer system.

1   78.   The method of Claim 77 wherein said verification data includes a

2   predetermined cipher text encrypted with an encryption key pair corresponding to

3   said second computer system.

1   79.   A computer system operable as a participant in a cluster of computer

2   systems providing a network service in response to network requests received from

3   host computer systems through a communications network, the cluster computer

4   systems interoperating to ensure the security and secure exchange of

5   configuration data in response to a single point secure administrative modification

6   of configuration data on any computer system of the cluster, said computer system

7   comprising:

8   a) a computer memory providing for the storage of configuration data

9   including a set of identifications of computer systems participating in a

10 preestablished computer system cluster;

11   b) a processor coupled to said computer memory and operative to execute

12 a control program that defines performance of a predetermined network service

13 in response to network requests as received from host computers, wherein

14 performance of said predetermined network service is controlled by said

15 configuration data;

16   c) an administrative interface coupled to said processor, wherein said

17 control program further enables secure performance of local administrative

18 modifications to said configuration data through said administrative interface;

19 and

20   d) a communications interface coupled to said processor and coupleable

21 to said preestablished computer system cluster, wherein said control program

22 further enables secure synchronization of said configuration data among said

23 computer system and said preestablished computer system cluster, said control

24 program limiting the transfer of said configuration data between said computer

25 system, as a first computer system, and a second computer system securely

26 matching a identification preexisting in said set of identifications.

1   80.   The computer system of Claim 79 wherein said configuration data is

2   transferred encrypted between said first computer system and said second

3   computer system and wherein the encryption of said configuration data is specific

4   to said first computer system and said second computer system.

1   81.   The computer system of Claim 80 wherein said processor is responsive to

2   a network synchronization message identifying a configuration data set more

3   recently modified relative to the configuration data stored in said computer

4   memory, said processor being operative to identify said second computer system

5   as the source of said network synchronization message, send a network

6   configuration data request message to said second computer system. receive, and

7   decrypt said configuration data set, and incorporate said configuration data set

8   into said computer memory.

1   82.   The computer system of Claim 81 wherein said processor is further

2   operative to validate said network synchronization message relative to said set of

3   identifications, prepare said network configuration data request to be validateable

4   against said set of identifications, and validate said configuration data set as

5   received against said set of identifications, whereby the transfer of said

6   configuration data set is secure and constrained with respect to said first computer

7   system to those computer systems of said preestablished computer system cluster

8   that are preexistingly identified by said set of identifications.